



## BGP 4 Prefix Filter and Inbound Route Maps

---

The BGP 4 Prefix Filter and Inbound Route Maps feature allows prefix-based matching support to the inbound neighbor route map. With this addition, an inbound route map can be used to enforce prefix-based policies.

- [Finding Feature Information, page 1](#)
- [Information About BGP 4 Prefix Filter and Inbound Route Maps, page 1](#)
- [How to Configure BGP 4 Prefix Filter and Inbound Route Maps, page 2](#)
- [Configuration Examples for BGP4 Prefix Filter and Inbound Route Maps, page 11](#)
- [Additional References for BGP Restart Neighbor Session After Max-Prefix Limit Reached, page 14](#)
- [Feature Information for BGP 4 Prefix Filter and Inbound Route Maps, page 15](#)

### Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

## Information About BGP 4 Prefix Filter and Inbound Route Maps

### BGP Policy Configuration

BGP policy configuration is used to control prefix processing by the BGP routing process and to filter routes from inbound and outbound advertisements. Prefix processing can be controlled by adjusting BGP timers, altering how BGP handles path attributes, limiting the number of prefixes that the routing process will accept, and configuring BGP prefix dampening. Prefixes in inbound and outbound advertisements are filtered using

route maps, filter lists, IP prefix lists, autonomous-system-path access lists, IP policy lists, and distribute lists. The table below shows the processing order of BGP policy filters.

**Table 1: BGP Policy Processing Order**

Inbound	Outbound
Route map	Distribute list
Filter list, AS-path access list, or IP policy	IP prefix list
IP prefix list	Filter list, AS-path access list, or IP policy
Distribute list	Route map

Whenever there is a change in the routing policy due to a configuration change, BGP peering sessions must be reset using the **clear ip bgp** command. Cisco software supports the following three mechanisms to reset BGP peering sessions:

- Hard reset—A hard reset tears down the specified peering sessions, including the TCP connection, and deletes routes coming from the specified peer.
- Soft reset—A soft reset uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reset uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply a new BGP policy without disrupting the network. Soft reset can be configured for inbound or outbound sessions.
- Dynamic inbound soft reset—The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for nondisruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh must first be advertised through BGP capability negotiation between peers. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

## How to Configure BGP 4 Prefix Filter and Inbound Route Maps

### Influencing Inbound Path Selection

BGP can be used to influence the choice of paths in another autonomous system. There may be several reasons for wanting BGP to choose a path that is not the obvious best route, for example, to avoid some types of transit traffic passing through an autonomous system or perhaps to avoid a very slow or congested link. BGP can influence inbound path selection using one of the following BGP attributes:

- AS-path

- Multi-Exit Discriminator (MED)

Perform one of the following tasks to influence inbound path selection:

## Influencing Inbound Path Selection by Modifying the AS\_PATH Attribute

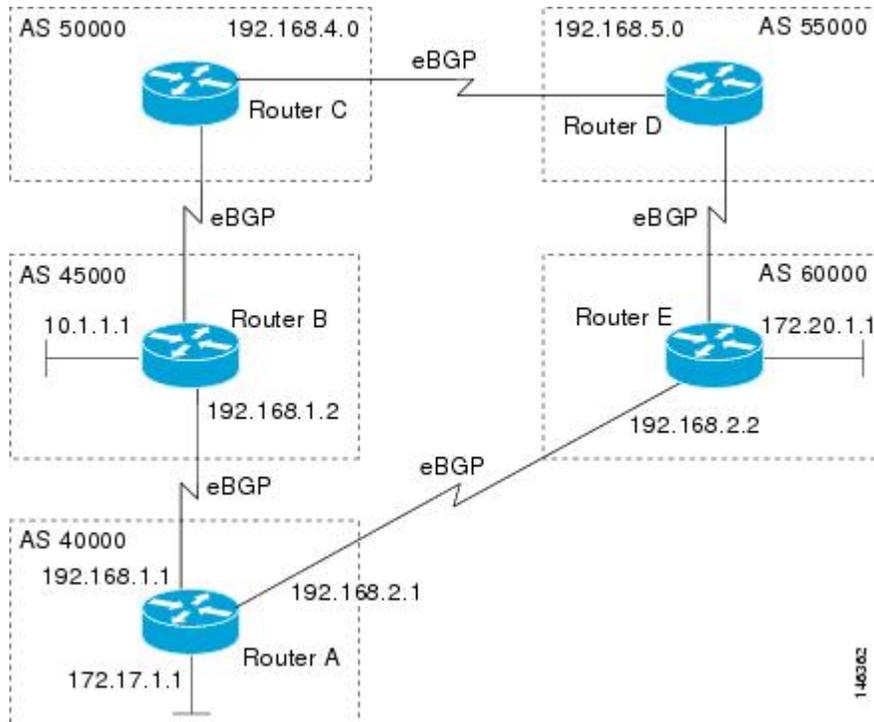
Perform this task to influence the inbound path selection for traffic destined for the 172.17.1.0 network by modifying the AS\_PATH attribute. The configuration is performed at Router A in the figure below. For a configuration example of this task using 4-byte autonomous system numbers in asplain format, see the “Example: Influencing Inbound Path Selection by Modifying the AS\_PATH Attribute Using 4-Byte AS Numbers”.

One of the methods that BGP can use to influence the choice of paths in another autonomous system is to modify the AS\_PATH attribute. For example, in the figure below, Router A advertises its own network, 172.17.1.0, to its BGP peers in autonomous system 45000 and autonomous system 60000. When the routing information is propagated to autonomous system 50000, the routers in autonomous system 50000 have network reachability information about network 172.17.1.0 from two different routes. The first route is from autonomous system 45000 with an AS\_PATH consisting of 45000, 40000, the second route is through autonomous system 55000 with an AS-path of 55000, 60000, 40000. If all other BGP attribute values are the same, Router C in autonomous system 50000 would choose the route through autonomous system 45000 for traffic destined for network 172.17.1.0 because it is the shortest route in terms of autonomous systems traversed.

Autonomous system 40000 now receives all traffic from autonomous system 50000 for the 172.17.1.0 network through autonomous system 45000. If, however, the link between autonomous system 45000 and autonomous system 40000 is a really slow and congested link, the **set as-path prepend** command can be used at Router A to influence inbound path selection for the 172.17.1.0 network by making the route through autonomous system 45000 appear to be longer than the path through autonomous system 60000. The configuration is done at Router A in the figure below by applying a route map to the outbound BGP updates to Router B. Using the **set as-path prepend** command, all the outbound BGP updates from Router A to Router B will have their AS\_PATH attribute modified to add the local autonomous system number 40000 twice. After the configuration, autonomous system 50000 receives updates about the 172.17.1.0 network through autonomous system 45000. The new AS\_PATH is 45000, 40000, 40000, and 40000, which is now longer than the AS-path from autonomous system 55000 (unchanged at a value of 55000, 60000, 40000). Networking devices in autonomous

system 50000 will now prefer the route through autonomous system 55000 to forward packets with a destination address in the 172.17.1.0 network.

**Figure 1: Network Topology for Modifying the AS\_PATH Attribute**



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. **exit-address-family**
10. **exit**
11. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
12. **set as-path** {**tag** | **prepend** *as-path-string*}
13. **end**
14. **show running-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Device# configure terminal	Enters global configuration mode.
Step 3	<b>router bgp</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config)# router bgp 40000	Enters router configuration mode for the specified routing process.
Step 4	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>autonomous-system-number</i>  <b>Example:</b> Device(config-router)# neighbor 192.168.1.2 remote-as 45000	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>• In this example, the BGP peer on Router B at 192.168.1.2 is added to the IPv4 multiprotocol BGP neighbor table and will receive BGP updates.</li> </ul>
Step 5	<b>address-family ipv4</b> [ <b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Device(config-router)# address-family ipv4 unicast	Specifies the IPv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>• The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>• The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>• The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<b>network</b> <i>network-number</i> [ <b>mask</b> <i>network-mask</i> ] <b>[route-map</b> <i>route-map-name</i> ]  <b>Example:</b> Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0	Specifies a network as local to this autonomous system and adds it to the BGP routing table. <ul style="list-style-type: none"> <li>• For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>

	Command or Action	Purpose
Step 7	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>  <b>Example:</b> <pre>Device(config-router-af)# neighbor 192.168.1.2 activate</pre>	Enables address exchange for address family IPv4 unicast for the BGP neighbor at 192.168.1.2 on Router B.
Step 8	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> <pre>Device(config-router-af)# neighbor 192.168.1.2 route-map PREPEND out</pre>	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named PREPEND is applied to outbound routes to Router B.</li> </ul>
Step 9	<b>exit-address-family</b>  <b>Example:</b> <pre>Device(config-router-af)# exit</pre>	Exits address family configuration mode and enters router configuration mode.
Step 10	<b>exit</b>  <b>Example:</b> <pre>Device(config-router)# exit</pre>	Exits router configuration mode and enters global configuration mode.
Step 11	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> <pre>Device(config)# route-map PREPEND permit 10</pre>	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named PREPEND is created with a permit clause.</li> </ul>
Step 12	<b>set as-path</b> { <i>tag</i>   <b>prepend</b> <i>as-path-string</i> }  <b>Example:</b> <pre>Device(config-route-map)# set as-path prepend 40000 40000</pre>	Modifies an autonomous system path for BGP routes. <ul style="list-style-type: none"> <li>Use the <b>prepend</b> keyword to prepend an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.</li> <li>In this example, two additional autonomous system entries are added to the autonomous system path for outbound routes to Router B.</li> </ul>
Step 13	<b>end</b>  <b>Example:</b> <pre>Device(config-route-map)# end</pre>	Exits route map configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
Step 14	<b>show running-config</b>  <b>Example:</b> Device# show running-config	Displays the running configuration file.

### Examples

The following partial output of the **show running-config** command shows the configuration from this task.

#### Router A

```
Device# show running-config
.
.
.
router bgp 40000
 neighbor 192.168.1.2 remote-as 45000
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 route-map PREPEND out
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
  exit-address-family
 !
 route-map PREPEND permit 10
  set as-path prepend 40000 40000
.
.
.
```

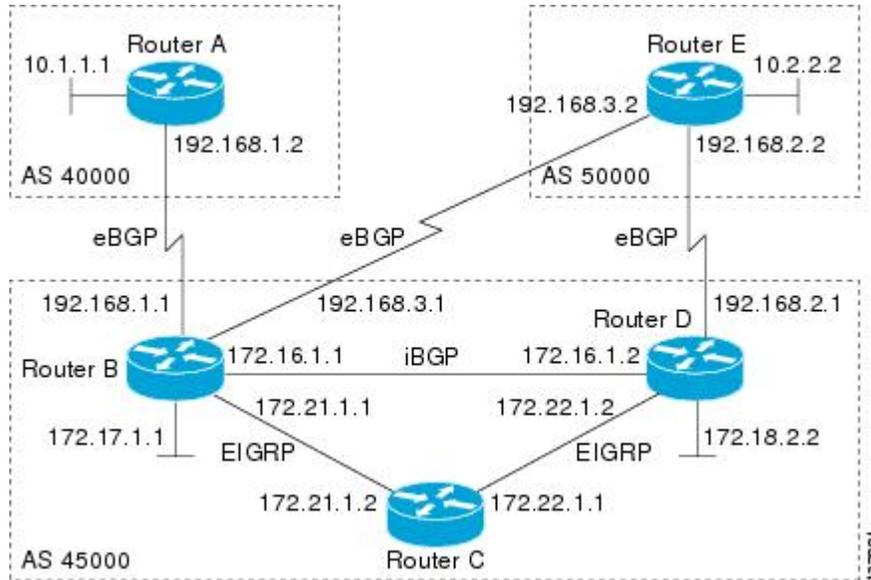
## Influencing Inbound Path Selection by Setting the MED Attribute

One of the methods that BGP can use to influence the choice of paths into another autonomous system is to set the Multi-Exit Discriminator (MED) attribute. The MED attribute indicates (to an external peer) a preferred path to an autonomous system. If there are multiple entry points to an autonomous system, the MED can be used to influence another autonomous system to choose one particular entry point. A metric is assigned using route maps where a lower MED metric is preferred by the software over a higher MED metric.

Perform this task to influence inbound path selection by setting the MED metric attribute. The configuration is performed at Router B and Router D in the figure below. Router B advertises the network 172.16.1.0 to its BGP peer, Router E in autonomous system 50000. Using a simple route map Router B sets the MED metric to 50 for outbound updates. The task is repeated at Router D but the MED metric is set to 120. When Router E receives the updates from both Router B and Router D the MED metric is stored in the BGP routing table. Before forwarding packets to network 172.16.1.0, Router E compares the attributes from peers in the same

autonomous system (both Router B and Router D are in autonomous system 45000). The MED metric for Router B is less than the MED for Router D, so Router E will forward the packets through Router B.

**Figure 2: Network Topology for Setting the MED Attribute**



Use the **bgp always-compare-med** command to compare MED attributes from peers in other autonomous systems.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
5. **address-family ipv4** [**unicast** | **multicast** | **vrf** *vrf-name*]
6. **network** *network-number* [**mask** *network-mask*] [**route-map** *route-map-name*]
7. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
8. **exit**
9. **exit**
10. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
11. **set metric** *value*
12. **end**
13. Repeat Step 1 through Step 12 at Router D.
14. **show ip bgp** [*network*] [*network-mask*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b></p> <pre>Device&gt; enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>Device# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><b>router bgp</b> <i>autonomous-system-number</i></p> <p><b>Example:</b></p> <pre>Device(config)# router bgp 45000</pre>	<p>Enters router configuration mode for the specified routing process.</p>
Step 4	<p><b>neighbor</b> <i>{ip-address   peer-group-name}</i> <b>remote-as</b> <i>autonomous-system-number</i></p> <p><b>Example:</b></p> <pre>Device(config-router)# neighbor 192.168.3.2 remote-as 50000</pre>	<p>Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router.</p>
Step 5	<p><b>address-family ipv4</b> [<b>unicast</b>   <b>multicast</b>   <b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router)# address-family ipv4 unicast</pre>	<p>Specifies the IPv4 address family and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>• The <b>unicast</b> keyword specifies the IPv4 unicast address family. By default, the router is placed in address family configuration mode for the IPv4 unicast address family if the <b>unicast</b> keyword is not specified with the <b>address-family ipv4</b> command.</li> <li>• The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>• The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>
Step 6	<p><b>network</b> <i>network-number</i> [<b>mask</b> <i>network-mask</i>] [<b>route-map</b> <i>route-map-name</i>]</p> <p><b>Example:</b></p> <pre>Device(config-router-af)# network 172.16.1.0 mask 255.255.255.0</pre>	<p>Specifies a network as local to this autonomous system and adds it to the BGP routing table.</p> <ul style="list-style-type: none"> <li>• For exterior protocols the <b>network</b> command controls which networks are advertised. Interior protocols use the <b>network</b> command to determine where to send updates.</li> </ul>

	Command or Action	Purpose
<b>Step 7</b>	<b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }  <b>Example:</b> <pre>Device(config-router-af)# neighbor 192.168.3.2 route-map MED out</pre>	Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>In this example, the route map named MED is applied to outbound routes to the BGP peer at Router E.</li> </ul>
<b>Step 8</b>	<b>exit</b>  <b>Example:</b> <pre>Device(config-router-af)# exit</pre>	Exits address family configuration mode and enters router configuration mode.
<b>Step 9</b>	<b>exit</b>  <b>Example:</b> <pre>Device(config-router)# exit</pre>	Exits router configuration mode and enters global configuration mode.
<b>Step 10</b>	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>sequence-number</i> ]  <b>Example:</b> <pre>Device(config)# route-map MED permit 10</pre>	Configures a route map and enters route map configuration mode. <ul style="list-style-type: none"> <li>In this example, a route map named MED is created.</li> </ul>
<b>Step 11</b>	<b>set metric</b> <i>value</i>  <b>Example:</b> <pre>Device(config-route-map)# set metric 50</pre>	Sets the MED metric value.
<b>Step 12</b>	<b>end</b>  <b>Example:</b> <pre>Device(config-route-map)# end</pre>	Exits route map configuration mode and enters privileged EXEC mode.
<b>Step 13</b>	Repeat Step 1 through Step 12 at Router D.	—
<b>Step 14</b>	<b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]  <b>Example:</b> <pre>Device# show ip bgp 172.17.1.0 255.255.255.0</pre>	(Optional) Displays the entries in the BGP routing table. <ul style="list-style-type: none"> <li>Use this command at Router E in the figure above when both Router B and Router D have configured the MED attribute.</li> <li>Only the syntax applicable to this task is used in this example. For more details, see the <i>Cisco IOS IP Routing: BGP Command Reference</i>.</li> </ul>

## Examples

The following output is from Router E in the figure above after this task has been performed at both Router B and Router D. Note the metric (MED) values for the two routes to network 172.16.1.0. The peer 192.168.2.1 at Router D has a metric of 120 for the path to network 172.16.1.0, whereas the peer 192.168.3.1 at Router B has a metric of 50. The entry for the peer 192.168.3.1 at Router B has the word `best` at the end of the entry to show that Router E will choose to send packets destined for network 172.16.1.0 via Router B because the MED metric is lower.

```
Device# show ip bgp 172.16.1.0

BGP routing table entry for 172.16.1.0/24, version 10
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
    1
  45000
    192.168.2.1 from 192.168.2.1 (192.168.2.1)
      Origin IGP, metric 120, localpref 100, valid, external
  45000
    192.168.3.1 from 192.168.3.1 (172.17.1.99)
      Origin IGP, metric 50, localpref 100, valid, external, best
```

# Configuration Examples for BGP4 Prefix Filter and Inbound Route Maps

## Example: Influencing Inbound Path Selection

The following example shows how you can use route maps to modify incoming data from a neighbor. Any route received from 10.222.1.1 that matches the filter parameters set in autonomous system access list 200 will have its weight set to 200 and its local preference set to 250, and it will be accepted.

```
router bgp 100
!
 neighbor 10.222.1.1 route-map FIX-WEIGHT in
 neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map FIX-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight 200
```

In the following example, the route map named FINANCE marks all paths originating from autonomous system 690 with an MED metric attribute of 127. The second permit clause is required so that routes not matching autonomous system path list 1 will still be sent to neighbor 10.1.1.1.

```
router bgp 65000
 neighbor 10.1.1.1 route-map FINANCE out
!
ip as-path access-list 1 permit ^690_
ip as-path access-list 2 permit .*
!
route-map FINANCE permit 10
 match as-path 1
 set metric 127
!
```

```
route-map FINANCE permit 20
  match as-path 2
```

Inbound route maps could perform prefix-based matching and set various parameters of the update. Inbound prefix matching is available in addition to autonomous system path and community list matching. The following example shows how the route map named SET-LOCAL-PREF sets the local preference of the inbound prefix 172.20.0.0/16 to 120:

```
!
router bgp 65100
  network 10.108.0.0
  neighbor 10.108.1.1 remote-as 65200
  neighbor 10.108.1.1 route-map SET-LOCAL-PREF in
!
route-map SET-LOCAL-PREF permit 10
  match ip address 2
  set local-preference 120
!
route-map SET-LOCAL-PREF permit 20
!
access-list 2 permit 172.20.0.0 0.0.255.255
access-list 2 deny any
```

## Example: Influencing Inbound Path Selection by Modifying the AS-path Attribute Using 4-Byte AS Numbers

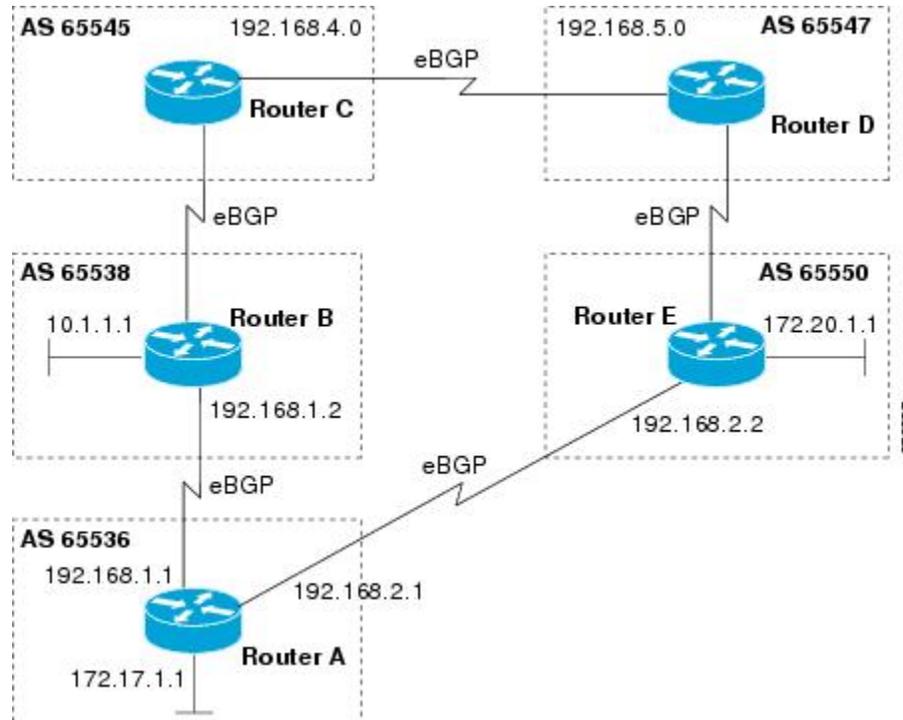
This example shows how to configure BGP to influence the inbound path selection for traffic destined for the 172.17.1.0 network by modifying the AS-path attribute. In Cisco IOS XE Release 2.4 and later releases, BGP support for 4-octet (4-byte) autonomous system numbers was introduced. The 4-byte autonomous system numbers in this example are formatted in the default asplain (decimal value) format; for example, Router B is in autonomous system number 65538 in the figure below.

One of the methods that BGP can use to influence the choice of paths in another autonomous system is to modify the AS-path attribute. For example, in the figure below, Router A advertises its own network, 172.17.1.0, to its BGP peers in autonomous system 65538 and autonomous system 65550. When the routing information is propagated to autonomous system 65545, the routers in autonomous system 65545 have network reachability information about network 172.17.1.0 from two different routes. The first route is from autonomous system 65538 with an AS-path consisting of 65538, 65536. The second route is through autonomous system 65547 with an AS-path of 65547, 65550, 65536. If all other BGP attribute values are the same, Router C in autonomous system 65545 would choose the route through autonomous system 65538 for traffic destined for network 172.17.1.0 because it is the shortest route in terms of autonomous systems traversed.

Autonomous system 65536 now receives all traffic from autonomous system 65545 for the 172.17.1.0 network through Router B in autonomous system 65538. If, however, the link between autonomous system 65538 and autonomous system 65536 is a really slow and congested link, the **set as-path prepend** command can be used at Router A to influence inbound path selection for the 172.17.1.0 network by making the route through autonomous system 65538 appear to be longer than the path through autonomous system 65550. The configuration is done at Router A in the figure below by applying a route map to the outbound BGP updates to Router B. Using the **set as-path prepend** command, all the outbound BGP updates from Router A to Router B will have their AS-path attribute modified to add the local autonomous system number 65536 twice. After the configuration, autonomous system 65545 receives updates about the 172.17.1.0 network through autonomous system 65538. The new AS-path is 65538, 65536, 65536, 65536, which is now longer than the AS-path from autonomous system 65547 (unchanged at a value of 65547, 65550, 65536). Networking devices in autonomous

system 65545 will now prefer the route through autonomous system 65547 to forward packets with a destination address in the 172.17.1.0 network.

**Figure 3: Network Topology for Modifying the AS-path Attribute**



The configuration for this example is performed at Router A in the figure above.

```
router bgp 65536
 address-family ipv4 unicast
  network 172.17.1.0 mask 255.255.255.0
  neighbor 192.168.1.2 remote-as 65538
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 route-map PREPEND out
 exit-address-family
 exit
 route-map PREPEND permit 10
 set as-path prepend 65536 65536
```

## Example: Filtering BGP Prefixes Using a Single Prefix List

The following example shows how a prefix list denies the default route 0.0.0.0/0:

```
ip prefix-list abc deny 0.0.0.0/0
```

The following example shows how a prefix list permits a route that matches the prefix 10.0.0.0/8:

```
ip prefix-list abc permit 10.0.0.0/8
```

The following example shows how to configure the BGP process so that it accepts only prefixes with a prefix length of /8 to /24:

```
router bgp 40000
 network 10.20.20.0
 distribute-list prefix max24 in
 !
 ip prefix-list max24 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

The following example configuration shows how to conditionally originate a default route (0.0.0.0/0) in RIP when a prefix 10.1.1.0/24 exists in the routing table:

```
ip prefix-list cond permit 10.1.1.0/24
 !
 route-map default-condition permit 10
 match ip address prefix-list cond
 !
 router rip
 default-information originate route-map default-condition
```

The following example shows how to configure BGP to accept routing updates from 192.168.1.1 only, besides filtering on the prefix length:

```
router bgp 40000
 distribute-list prefix max24 gateway allowlist in
 !
 ip prefix-list allowlist seq 5 permit 192.168.1.1/32
 !
```

The following example shows how to direct the BGP process to filter incoming updates to the prefix using name1, and match the gateway (next hop) of the prefix being updated to the prefix list name2, on Gigabit Ethernet interface 0/0/0:

```
router bgp 103
 distribute-list prefix name1 gateway name2 in gigabitethernet 0/0/0
```

## Additional References for BGP Restart Neighbor Session After Max-Prefix Limit Reached

### Related Documents

Related Topic	Document Title
Cisco IOS commands	<a href="#">Cisco IOS Master Command List, All Releases</a>
BGP commands	<a href="#">Cisco IOS IP Routing: BGP Command Reference</a>

### Standards and RFCs

Standard/RFC	Title
RFC 2918	<i>Route Refresh Capability for BGP-4</i>

Standard/RFC	Title
RFC 4486	<i>Subcodes for BGP Cease Notification Message</i>

#### Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for BGP 4 Prefix Filter and Inbound Route Maps

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 2: Feature Information for BGP 4 Prefix Filter and Inbound Route Maps**

Feature Name	Releases	Feature Information
BGP 4 Prefix Filter and Inbound Route Maps	Cisco IOS XE Release 3.1.0SG Cisco IOS XE Release 3.2SE Cisco IOS XE Release 3.3SE	The BGP 4 Prefix Filter and Inbound Route Maps feature allows prefix-based matching support to the inbound neighbor route map. With this addition, an inbound route map can be used to enforce prefix-based policies.  In Cisco IOS XE Release 3.3SE, support was added for the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches.

